## CLAIMS

1. A security device comprising two or more magnetic elements, wherein said magnetic elements are responsive to an applied magnetic field to provide a characteristic response.

2. The security device of Claim 1, wherein said characteristic response is provided in combination with a premeasured characteristic response.

3. The security device of Claim 1 or Claim 2, wherein said characteristic response represents an aggregate response of said magnetic elements to said applied magnetic field.

4. The security device of any preceding Claim, wherein said magnetic elements are supported by a substrate.

5. The security device of Claim 4, wherein said magnetic elements are supported on said substrate.

6. The security device of any preceding Claim, wherein the magnetic elements comprise thin layer magnetic material.

7. The security device of Claim 6, wherein the thin layers of magnetic material are less than 1 μm thick.

8. The security device of Claim 7, wherein the thin layers of magnetic material between 10 nm and 100 nm thick.

9. The security device of any preceding Claim, wherein said magnetic elements are responsive to said applied magnetic field to switch the magnetisation or magnetic polarisation of at least one of the magnetic elements.

10. The security device of any preceding Claim, wherein at least one of the magnetic elements is made from a magnetically soft material.

11. The security device of Claim 10, wherein at least one of the magnetic elements comprises a magnetically soft material selected from one or more of: nickel, iron, cobalt and alloys thereof with each other or silicon, such as nickel iron alloy, cobalt iron alloy, iron silicon alloy or cobalt silicon alloy.

12. The security device of Claim 10 or 11, wherein said magnetically soft material is a permalloy material.

13. The security device of any preceding Claim, wherein at least one of the magnetic elements is substantially wire-shaped or flattened wire shaped.

14. The security device of any preceding Claim, wherein the device comprises a generally parallel array of elongate rectangular magnetic elements.

15. The security device of Claim 14, wherein the magnetic elements comprise an array of generally parallel magnetic nanowires.

16. The security device of any preceding Claim, wherein the magnetic elements have generally the same size and/or shape.

17. The security device of any preceding Claim, wherein several discrete groups of differently sized and/or shaped magnetic elements, the magnetic elements being generally similarly sized and/or shaped within each group, are provided so that several different switching fields can be identified.

18. The security device of Claim 17, comprising an ensemble of rectangular magnetic elements in parallel array including several discrete groups of magnetic elements of different widths.

19. The security device of any preceding Claim, wherein differently sized and/or shaped magnetic elements are provided in a continuously varying array, so that variations in sized and/or shape between a magnetic element and its neighbours are minimised to avoid large discontinuities.

20. The security device of Claim 19, comprising an ensemble of rectangular magnetic elements in parallel array of width varying continuously across the array.

21. The security device of any preceding Claim, further comprising a single relatively large area magnetic element for use as a reference element.

22. The security device of any preceding Claim, wherein at least one of the magnetic elements is backed by a light reflective layer.

23. The security device of any preceding Claim, wherein at least one of the magnetic elements is provided proximal a reduced light reflectivity portion of said security device.

24. The security device of any preceding Claim, wherein the magnetic elements are arranged to provide a linear pattern.

25. The security device of any preceding Claim, wherein said magnetic elements are arranged to provide a two-dimensional pattern.

26. The security device of any preceding Claim, further comprising a unique identifier incorporated therewith.

27. The security device of claim 26, wherein said unique identifier is provided by way of one or more of: an optically readable bar code; one or more optical indicia; a magnetically encoded identifier; and an electronic identifier.

28. The security device of claim 27, mounted upon a smart-card, wherein said electronic identifier is provided by a smart-card chip provided on said smart-card.

29. The security device of any preceding Claim, wherein premeasured characteristic response information representing one or more measurable parameters of said characteristic response is stored on said security device.

30. The security device of Claim 29, wherein said premeasured characteristic response information is in encrypted form.

31. The security device of Claim 30, wherein said premeasured characteristic response information is encrypted using an asymmetric encryption algorithm with the private key used for enciphering being kept

secret and the public key used for deciphering being made available to any reader of the security device.

32. The security device of Claim 2 or any one of Claims 3 to 31 when dependent on Claim 2, wherein the premeasured characteristic response is stored in physical proximity to the security device in machine-readable form.

33. A method of manufacturing a security device, comprising:

providing two or more magnetic elements, wherein said magnetic elements provide a characteristic response in response to an applied magnetic field.

34. The method of Claim 33, comprising providing said magnetic elements on a substrate.

35. The method of Claim 33 or Claim 34, comprising forming at least one of the magnetic elements using a lift off or wet etching process.

36. The method of Claim 33 or Claim 34, comprising forming at least one of the magnetic elements using an ion beam etching process.

37. The method of any one of Claims 33 to 36, comprising measuring the magnitude(s) of one or more magnetic parameters of said magnetic elements.

38. The method of Claim 37, comprising measuring one or more of coercivity and jitter values.

39. The method of Claim 37 or Claim 38, comprising using the measured magnitude(s) of said one or more magnetic parameters to represent premeasured characteristic response information.

40. The method of Claim 39, comprising encrypting said premeasured characteristic response information.

41. The method of Claim 39 or Claim 40, comprising storing said premeasured characteristic response information in encrypted or unencrypted form on said security device.

42. The method of Claim 39 or Claim 40, comprising storing said premeasured characteristic response information in encrypted or unencrypted form in a storage medium remote from said security device.

43. The method of Claim 42, comprising storing said premeasured characteristic response information in encrypted or unencrypted form in a database.

44. The method of any one of Claims 33 to 43, further comprising providing said security device with a unique identifier.

45. The method of Claim 44 when dependant upon any one of Claims 39 to 43, comprising storing a representation of said unique identifier in association with said premeasured characteristic response information.

46. A system for reading a security device, comprising:

a magnetic field generation system for applying a magnetic field to a security device comprising two or more magnetic elements; and

a detection system for measuring one or more parameters representative of a measured characteristic response of said security device in response to said magnetic field,

wherein said system is operable to compare said one or more parameters representative of a measured characteristic response to one or more respective parameters of a premeasured characteristic response to determine whether respective measured and premeasured parameters are substantially equivalent.

47. The system of Claim 46, wherein said measured characteristic response and said premeasured characteristic response are representative of an aggregate response produced by said two or more magnetic elements.

48. The system of Claim 46 or Claim 47, wherein the magnetic field generation system is operable to apply a time varying magnetic field to a security device.

49. The system of any one of Claims 46 to 48, wherein a light beam is used to interrogate said security device.

50. The system of Claim 49, wherein said light beam is a visible or near-infrared beam produced by a laser diode.

51. The system of any one of Claims 46 to 50, wherein said parameters represent one or more of coercivity and jitter values.

52. The system of any one of Claims 49 to 51, wherein said detection system incorporates magneto-optic Kerr effect detection apparatus for

detecting changes induced in said light beam by magnetic elements of said security device.

53. The system of Claim 52, wherein said magneto-optic Kerr effect detection apparatus is configured to operate in transverse mode.

54. The system of any one of Claims 36 to 40, further operable to deflect said light beam across the surface of said security device.

55. The system of any one of Claims 46 to 54, further operable to read a unique identifier from said security device.

56. The system of Claim 55, wherein said unique identifier is identified by reading one or more of: an optically readable bar code; one or more optical indicia; a magnetically encoded identifier; and an electronic identifier.

57. The system of any one of Claims 46 to 56, further operable to determine said one or more respective parameters of the premeasured characteristic response by reading said one or more parameters from said security device.

58. The system of any one of Claims 46 to 57, further operable to determine said one or more respective parameters of the premeasured characteristic response by reading said one or more parameters from a database.

59. The system of Claim 58, wherein said database is remotely located from said detection system.

60. The system of any one of Claims 46 to 59, further operable to decrypt premeasured characteristic response information where it is read or provided in encrypted form.

61. A method for reading a security device, comprising:

applying a magnetic field to a security device comprising two or more magnetic elements;

measuring one or more parameters representative of a measured characteristic response of said security device in response to said magnetic field; and

comparing said one or more parameters representative of a measured characteristic response to one or more respective parameter(s) of a premeasured characteristic response to determine whether respective measured and premeasured parameters are substantially equivalent.

62. The system of Claim 61, wherein said measured characteristic response and said premeasured characteristic response are representative of an aggregate response produced by said two or more magnetic elements.

63. The method of Claim 61 or Claim 62, comprising applying a time varying magnetic field to a security device.

64. The method of any one of Claims 61 to 63, wherein measuring of one or more parameters representative of a measured characteristic response of said security device in response to said magnetic field comprises measuring one or more of coercivity and jitter values.

65. The method of any one of Claims 61 to 64, comprising interrogating said security device using a light beam.

66. The method of any one of Claims 61 to 65, comprising operating a laser to produce a visible or near-infrared beam.

67. The method of Claim 65 or Claim 66, comprising detecting changes induced in said light beam by magnetic elements of said security device using the magneto-optic Kerr effect.

68. The method of Claim 67, comprising using the magneto-optic Kerr effect transverse mode.

69. The method of any one of Claims 61 to 68, comprising reading a unique identifier from said security device.

70. The method of Claim 69, comprising identifying said unique identifier by reading one or more of: an optically readable bar code; one or more optical indicia; a magnetically encoded identifier; and an electronic identifier.

71. The method of any one of Claims 61 to 70, comprising determining said respective one or more parameters of the premeasured characteristic response by reading said one or more parameters from said security device.

72. The method of any one of Claims 61 to 71, comprising determining said one or more respective parameters of the premeasured characteristic response by reading said one or more parameters from a database.

73. The method of Claim 72, comprising accessing a database remotely located from said detection system.

74. The method of any one of Claims 61 to 73, further comprising decrypting premeasured characteristic response information where it is read or provided in encrypted form.

75. A product comprising the security device of any one of Claims 1 to 32.

76. The product of Claim 75, comprising one or more of: a document; a passport; an identity card; a compact disc; a digital versatile disc; a software product; packaging; an item of clothing; an item of footwear; a smart-card; a credit or bank card; a cosmetic item; an engineering part; an accessory; and any other goods and/or items of commerce, whether manufactured or otherwise.